REMARKS

Applicants wish to thank the Examiner for considering the present application. In the Final Office Action dated February 10, 2006, Claims 1-23 are pending in the application. Applicants respectfully request the Examiner for a reconsideration of the rejections.

Claims 1-23 stand rejected under 35 U.S.C. §112, second paragraph, for containing various errors. Applicants have revised the claims and believe that the errors have been overcome.

Claims 1-23 stand rejected under 35 U.S.C. §103(a) as being unpatentable over *Grantges* (6,324,648) in view of *Wood* (6,609,198). Applicants respectfully traverse.

The Examiner first focuses on Claim 8. Claim 8 recites a method of authenticating a user having a user privilege server proxy for a network system having a privilege server, a headend server, and a web adapter. One of the steps is that when a user is validated at the privilege server, generating a ticket for the user at the privilege server, encrypting the ticket with a user password to form a user encrypted ticket and providing the encrypted ticket to the user privilege server proxy through the headend server and decrypting the encrypted ticket. The Examiner points to Col. 7, line 63 to Col. 8, line 14. Although encryption of a digital certificate is set forth, no teaching or suggestion is provided in this passage for encrypting the ticket with a user password to form an encrypted ticket. Only a user's public key is set forth and not a password. Further, the Examiner recognizes that the *Grantges* reference does not disclose forming a packet having a sequence number and a session key encrypted with the ticket at the privilege server or decrypting this packet. The Examiner points to the *Wood* reference, Col. 12, line 52, to Col. 13, line 10, for forming a packet having a sequence number and a session key encrypted with the ticket at the privilege server. Applicants can find no teaching or suggestion in Col. 13 for encrypting anything, let alone the sequence number and session key. Applicants therefore respectfully request the Examiner to reconsider the rejection.

As those skilled in the art will recognize, the present system does not rely on a cookie-based system that are maintained by browsers as is set forth in both the

Wood and *Grantges* references. The ticket mechanism set forth in the present invention ensures security is dynamically modified by the client system with each request. This ticket when passed on to the server is validated based upon initial ticket generated by an authentication server as well as the ticket received from the client system. The system helps provide security against man in the middle attacks or packet resend attacks even in the absence of SSL security between a server and client. The ticket-based system of the present invention allows E-learning applications that require low latency for interactive multimedia applications like video conversation to be secure and scalable. Clock synchronization is important in the systems described in the *Wood* and *Grantges* references. The present invention does not depend on clock synchronization and thus can be distributed systems across the internet. Also, heterogeneous application environments are supported with a ticket-based mechanism that go beyond HTTP. That is, the present invention is not limited to HTTP type protocol. The present invention also provides a method for authenticating two untrusted domains to share security credentials of a single client and provide single secure logon by a client in multiple domains.

Claim 1 also recites similar limitations with respect to forming a packet having a sequence number session key and the ticket at the privilege server. As mentioned above in Claim 8, no teaching or suggestion is provided for this in either reference.

In the Final Office Action, the Examiner does not understand the encryption. Those skilled in the art will recognize that various types of encryption may take place. The use of a password or a session key encrypted with something else such as a ticket or a password is well known in the art. The “encrypted with” language merely means the encryption has within it the specific part such as the ticket or password or the like. The “encrypted with” language is not a special type of algorithm beyond mere encryption. Rather, the language sets forth what is included in the encryption. Applicants therefore do not agree that the combination of the *Grantges* and *Wood* references teach or suggest setting the ticket and sequence number encrypted with the session key to a service server as recited in Claim 1. Likewise, Applicants do not believe that the combination teaches encrypting the ticket with a user password to

form an encrypted ticket as recited in Claim 8. Also, the combination does not teach or suggest a packet having a sequence number and a session key encrypted with a ticket at the privilege server. Likewise, the combination also does not teach or suggest encrypting the session key and sequence number with a ticket to form a packet as set forth in Claim 12. Claim 23 also recites encrypting a ticket with a user password to form an encrypted ticket. As mentioned above, this is not set forth in either of the *Grantges* or *Wood* references.

Likewise, Claims 12, 13 and 23 include similar limitations and therefore are also believed to be allowable for the same reasons set forth above. Likewise, the dependent claims are also believed to be allowable for the same reasons set forth above.

In light of the above remarks, Applicants submit that all objections and rejections are now overcome. The application is now in condition for allowance and expeditious notice thereof is earnestly solicited. Should the Examiner have any questions or comments the Examiner is respectfully requested to call the undersigned attorney.

Please charge any fees required in the filing of this amendment to Deposit Account 50-0476.

Respectfully submitted,

ARTZ & ARTZ, PC

Kevin G. Mierzwa
Registration No. 38,049
28333 Telegraph Road, Suite 250
Southfield, MI 48034
(248) 223-9500

Date: March 22, 2006